Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	DA 11-131
Unlicensed Operation in the TV Broadcast Bands	)	DA 09-2479
	)	ET Docket No. 04-186
Additional Spectrum for Unlicensed Devices Below 900 MHz and in the 3 GHz Band	)	ET Docket No. 02-380

To: Marlene H. Dortch
Office of the Secretary, Federal Communications Commission

SUPPLEMENT TO
COMSEARCH PROPOSAL
TO BE DESIGNATED AS A
TV BAND DEVICE DATABASE MANAGER

In response to the above-mentioned Order[1] from the Federal Communications Commission's Office of Engineering and Technology (OET) issued January 26, 2011, Comsearch hereby submits this supplement to our proposal to develop and manage an independent TV Band Device Database.[2] In addition, we hereby indicate the undersigned as the responsible party who will represent Comsearch at the workshops and also ensure compliance with all of the conditions in the *Order*.

[1] See Order ET Docket No. 04-186 (DA 11-131) 26 FCC Rcd 554 (2011) (*Order*);and *Office of Engineering and Technology Invites Proposals from Entities Seeking to be Designated TV Band Device Database Managers*, ET Docket No. 04-186 (DA 09-2479) (*Public Notice*) 23 FCC Rcd 16807 (2008); and *Second Report and Order and Memorandum Opinion and Order,* (Second MO&O) ET Docket No. 04-186, ET Docket No. 02-380, 23 FCC Rcd 16807 (2008).
[2] See *Comsearch Proposal To Be Designated As A TV Band Device Database Manager*, January 4, 2010.

1. Introduction

Comsearch is pleased to be selected as a TV bands device database administrator, albeit conditionally. Given our experience detailed in our proposal, we understand and appreciate the complexities associated with bringing the TV Bands Database online. We believe our initial proposal in concert with this supplement will help to underscore our ability to help bring about the success of database-enabled cognitive radio particularly for TV white space.

The *Order* directs each of the database administrators to supplement previous filings with sufficient detailed information to indicate how they will comply with the rule changes adopted in the *Second MO&O*.[3] We note that there have been five Petitions for Reconsideration filed in the proceeding seeking to affect changes to the changed rules.[4] In addition, there are numerous efforts under way to standardize the database interfaces and security.[5] Comsearch is participating in as many of these efforts as possible in an attempt to develop comprehensive yet flexible requirements to support an ecosystem of unlicensed devices that has never been created. Further, the Commission has indicated they plan to have significant database oversight and testing to the extent that they will conduct a series of mandatory workshops, they will identify the tasks that each administrator will have to perform to show compliance with the rules, and they will require real-world testing.[6] Accordingly, we believe there will be adequate opportunity to *demonstrate* compliance with the Commission's rules sufficient to be designated unconditionally as a TV bands device database administrator. However, we state categorically that Comsearch will comply with all Commission rules, and that we will not use our capacity as

[3] See *Order* at ¶19.
[4] See Report No. 2924, *Petitions For Reconsideration Of Action In Rulemaking Proceeding*, February 2, 2011.
[5] IEEE 802.11af is working on the database-device interface and associated security issues. The Wi-Fi Alliance is working to develop test plans, specification and a certification program for TV White Spaces devices based on the IEEE 802.11af standard. The Wireless Innovation Forum is working on a database interface specification effort that includes security. The Internet Engineering Technology Forum (IETF) is working on whitespace database queries.
[6] *Order* at ¶9.

a database manager to engage in any discriminatory or anti-competitive practices or practices that may compromise the privacy of users.

2. Compliance Matrix

Comsearch has identified the following changes that will impact us as a TV bands database administrator and we address our compliance in the following Compliance Matrix:

Comsearch Compliance with FCC Rules, Part 15, Subpart H as Changed in the *Second MO&O*		
Rule Section	**Change or New Requirement**	**Comsearch Response**
§15.707(a) Permissible channels of operation	All TVBDs are permitted to operate available channels in the frequency bands 512-608 MHz (TV channels 21-36) and 614-698 MHz (TV channels 38-51), subject to the interference protection requirements in §§ 15.711 and 15.712, except that operation of TVBDs is prohibited on the first channel above and the first channel below TV channel 37 (608-614 MHz) that are available, *i.e.*, not occupied by an authorized service. If a channel is not available both above and below channel 37, operation is prohibited on the first two channels nearest to channel 37. These channels will be identified and protected in the TV bands database(s).	In the development of our channel availability algorithms, we have ensured that the proper channels are selected for use by TVBDs in accordance with this and other applicable rule sections.
§15.709(b)(2) Antenna requirements	Fixed devices may not be located at sites where the height above average terrain (HAAT) at ground level is more than 76 meters. The ground level HAAT is to be calculated by the TV bands database that the device contacts for available channels using computational software employing the methodology in section 73.684(d) of this chapter.	We have implemented the appropriate calculation of HAAT at ground level consistent with §73.684(d), and send “no channels available” commands to all Fixed TVBD operation above 76 meters.

Comsearch Compliance with FCC Rules, Part 15, Subpart H as Changed in the *Second MO&O*		
Rule Section	**Change or New Requirement**	**Comsearch Response**
§15.711(b)(3)(vi) Geo-location and database access requirements	TV band devices shall incorporate adequate security measures to ensure that they are capable of communicating for purposes of obtaining lists of available channels only with databases operated by administrators authorized by the Commission, and to ensure that communications between TV band devices and databases between TV band devices are secure to prevent corruption or unauthorized interception of data. This requirement includes implementing security for communications between Mode I personal portable devices and fixed or Mode II devices for purposes of providing lists of available channels.	In our response to Question 5 of the Public Notice, we described our approach to security.[7] [8] For convenience, we have included this section from our response in its entirety in the Appendix. We maintain that our approach is still consistent with this requirement, but we also understand security requirements are subject to change as device interfaces and security threats are better defined in concert with numerous (and overlapping) industry standardization efforts. We will make all appropriate modifications to our security approach consistent with requirements.
§15.711(f) Security	(i) For purposes of obtaining a list of available channels and related matters, fixed and Mode II TVBDs shall only be capable of contacting databases operated by FCC designated administrators.	
	(ii) Communications between TV bands devices and TV bands databases are to be transmitted using secure methods that ensure against corruption or unauthorized modification of the data; this requirement applies to communications of channel availability and other spectrum access information between fixed and Mode II devices (it is not necessary for TVBDs to apply security coding to channel availability and channel access information where they are not the originating or terminating device and that they simply pass through).	

[7] See *Public Notice* at Question 5.
[8] See Comsearch *Proposal* pp 38 – 42.

Comsearch Compliance with FCC Rules, Part 15, Subpart H as Changed in the *Second MO&O*		
Rule Section	**Change or New Requirement**	**Comsearch Response**
	(iii) Communications between a Mode I device and a fixed or Mode II device for purposes of obtaining a list of available channels shall employ secure methods that ensure against corruption or unauthorized modification of the data. When a Mode I device makes a request to a fixed or Mode II device for a list of available channels the receiving device shall check with TV bands database that the Mode I device has a valid FCC Identifier before providing a list of available channels. Contact verification signals transmitted for Mode I devices are to be encoded with encryption to secure the identity of the transmitting device. Mode I devices using contact verification signals shall accept as valid for authorization only the signals of the device from which they obtained their list of available channels.	Please see previous discussion regarding security under §15.711(b)(3)(vi) - Geo-location and database access requirements. We will verify that a TVBD requesting access to the database has a valid FCC Identifier before providing a list of available channels. We understand that the Commission's Equipment Authorization System database may not be available for downloading.[9] We are eager to work with the Commission to understand how data on FCC-certified TVBDs will be made available to TV bands database administrators.
	(iv) A TV bands database shall be protected from unauthorized data input or alteration of stored data. To provide this protection, the administrator of the TV bands database administrator shall establish communications authentication procedures that allow the fixed or Mode II devices to be assured that the data they receive is from an authorized source.	Please see previous discussion regarding security under §15.711(b)(3)(vi) - Geo-location and database access requirements.
	(v) Applications for certification of TV bands devices are to include a high level operational description of the technologies and measures that are incorporated in the device to comply with the security requirements of this section. In addition, applications for certification of fixed and Mode II devices are to identify at least one of the TV bands databases operated by a designated TV bands database administrator that the device will access for channel availability and affirm that the device will conform to the communications security methods used by that database.	Please see previous discussion regarding security under §15.711(b)(3)(vi) - Geo-location and database access requirements. We are working with TVBD manufacturers to develop device/database certification requirements.
§15.712(f) Interference protection requirements. - Low power auxiliary services, including wireless microphones:	(1) Fixed TVBDs are not permitted to operate within 1 km, and personal/portable TVBDs will not be permitted to operate within 400 meters, of the coordinates of registered low power auxiliary station sites on the registered channels during the designated times they are used by low power auxiliary stations.	In the development of our channel availability algorithms, we have ensured that the proper channels are selected for use by TVBDs in accordance with this rule section.

[9] Private communications with the Commission's Office of Engineering and Technology.

Comsearch Compliance with FCC Rules, Part 15, Subpart H as Changed in the *Second MO&O*		
Rule Section	**Change or New Requirement**	**Comsearch Response**
§15.712(f) Interference protection requirements. - Border areas near Canada and Mexico:	Fixed and personal/portable TVBDs shall comply with the required separation distances in §15.712(a)(2) from the protected contours of TV stations in Canada and Mexico. TVBDs are not required to comply with these separation distances from portions of the protected contours of Canadian or Mexican TV stations that fall within the United States.	We have made the appropriate modifications to our channel availability algorithms to comply with this rule section.
§15.713(a) TV bands database	A database must provide fixed and Mode II personal portable TVBDs with channel availability information that includes scheduled changes in channel availability over the course of the 48 hour period beginning at the time the TVBDs make a re-check contact.	As part of the channel availability dataset provided to TVBDs, we will include scheduled changes in channel availability over the course of the 48 hour period beginning at the time the TVBDs make a re-check contact. However, we also note that particular use cases and TVBD interfaces are still under development.
	In making lists of available channels available to a TVBD, the TV bands database shall ensure that all communications and interactions between the TV bands database and the TVBD include adequate security measures such that unauthorized parties cannot access or alter the TV bands database or the list of available channels sent to TVBDs or otherwise affect the database system or TVBDs in performing their intended functions or in providing adequate interference protections to authorized services operating in the TV bands.	Please see previous discussion regarding security under §15.711(b)(3)(vi) - Geo-location and database access requirements.
	A TV bands database must also verify that the FCC identifier (FCC ID) of a device seeking access to its services is valid; under this requirement the TV bands database must also verify that the FCC ID of a Mode I device provided by a fixed or Mode II device is valid. A list of devices with valid FCC IDs and the FCC IDs of those devices is to be obtained from the Commission's Equipment Authorization System.	We will verify that a TVBD requesting access to the database has a valid FCC Identifier before providing a list of available channels. We understand that the Commission's Equipment Authorization System database may not be available for downloading. We are eager to work with the Commission to understand how data on FCC-certified TVBDs will be made available to TV bands database administrators.
§15.713(e) TV bands database - TVBD initialization	(5) A fixed or Mode II TVBD that provides a list of available channels to a Mode I device shall notify the database of the FCC identifier of such Mode I device and receive verification that that FCC identifier is valid before providing the list of available channels to the Mode I device.	Please see previous discussion under §15.713(a), TV bands database, regarding use and access of the Commission's EAS database.

Comsearch Compliance with FCC Rules, Part 15, Subpart H as Changed in the *Second MO&O*		
Rule Section	**Change or New Requirement**	**Comsearch Response**
§15.713(e) TV bands database - TVBD initialization	(6) A fixed device located at a site where the ground level height above average terrain (HAAT) is greater than 76 meters shall not be provided a list of available channels. The ground level HAAT of sites occupied by fixed TVBDs is to be calculated using computational software employing the methodology in section 73.684(d) of this chapter	Please see previous discussion under §15.709(b)(2) Antenna requirements.
§15.713 TV bands database - TV bands database information	(9) Unlicensed wireless microphones at venues of events and productions/shows that use large numbers of wireless microphones that cannot be accommodated in the two reserved channels and other channels that are not available for use by TVBDs at that location. Sites of eligible event venues using unlicensed wireless microphones must be registered with the Commission at least 30 days in advance of the defined time of operation and the Commission will provide this information to the data base managers.	We will modify our data structures to accommodate this data. We are eager to work with the Commission to understand how this data will be made available.

Comsearch Compliance with FCC Rules, Part 15, Subpart H as Changed in the *Second MO&O*		
Rule Section	**Change or New Requirement**	**Comsearch Response**
§15.713 (j) TV bands database - Security	The TV bands database shall employ protocols and procedures to ensure that all communications and interactions between the TV band database and TVBDs are accurate and secure and that unauthorized parties cannot access or alter the database or the list of available channels sent to a TVBD. (1) Communications between TV band devices and TV bands databases, and between different TV bands databases, shall be secure to prevent corruption or unauthorized interception of data. A TV bands database shall be protected from unauthorized data input or alteration of stored data. (2) A TV bands database shall verify that the FCC identification number supplied by a fixed or personal/portable TV band device is for a certified device and may not provide service to an uncertified device. (3) A TV bands database must not provide lists of available channels to uncertified TV bands devices for purposes of operation (it is acceptable for a TV bands database to distribute lists of available channels by means other than contact with TVBDs to provide list of channels for operation). To implement this provision, a TV bands database administrator shall obtain a list of certified TVBDs from the FCC Equipment Authorization System.	Please see previous discussion regarding security under §15.711(b)(3)(vi) - Geo-location and database access requirements. Please also see previous discussion under §15.713(a), TV bands database, regarding use and access of the Commission's EAS database.
§15.715 TV bands database administrator	(e) Provide accurate lists of available channels to fixed and personal/portable TVBDs that submit to it the information required under §§ 15.713(e), (f), and (g) based on their geographic location and provide accurate lists of available channels to fixed and Mode II devices requesting lists of available channels for Mode I devices. Database administrators may allow prospective operators of TV bands devices to query the database and determine whether there are vacant channels at a particular location.	We will ensure accurate channel availability results consistent with the Commission's database certification procedures. All prospective operators of TVBDs will be allowed to query the database and determine whether there are vacant channels at a particular location.
	(f) Establish protocols and procedures to ensure that all communications and interactions between the TV band database and TVBDs are accurate and secure and that unauthorized parties cannot access or alter the database or the list of available channels sent to a TVBD consistent with the provisions of Section 15.713(i).	Please see previous discussion regarding security under §15.711(b)(3)(vi) - Geo-location and database access requirements. Please also see previous discussion regarding §15.715(e) TV bands database administrator.

3. Conclusions

Comsearch is pleased to be designated as a TV bands device database administrator, if only conditionally. We understand and appreciate that this is a complicated and untrodden path. We also understand that the Commission has identified several waypoints to ensure the databases successfully and securely communicate with each other, with the Commission, and with TVBDs while providing accurate lists of available channels. We believe our experience in concert with all stakeholders under the Commission's leadership will help to bring about the success of database enabled cognitive radios for broadband wireless devices in the TV spectrum.

Respectfully Submitted,

/s/ H. Mark Gibson

H. Mark Gibson
Sr. Director, Regulatory Policy
COMSEARCH
19700 Janelia Farm Boulevard
Ashburn, Virginia 20147

Date: February 28, 2011

cc: Hugh L. Van Tuyl
Office of Engineering and Technology
Federal Communications Commission

APPENDIX

Excerpt From Comsearch Proposal to be Designated as a TV Band Device Database Manager

[Security]
5-a) The entity must describe the methods (e.g., interfaces, protocols) that will be used by TV band devices to communicate with the database and the procedures, if any, that it plans to use to verify that a device can properly communicate with the database.

Comsearch employs technical expertise to integrate any type of security protocol for the communication of the white space device with the database. There are many secure protocols that can be deployed on the OSI Seven Layer Model. The layered approach will ensure secure communication between the WSD and the database as well as safeguarding the integrity of the database, web servers, and network from criminal or improper activity. The specific security methods that meet the device manufacturer and our database requirements have yet to be determined. However, we will deploy security methods that meet industry standards.

Device manufacturers will create a secure account with the database via web server. Comsearch will deploy encryption policies (e.g., TLS) for the transfer of data between the manufacturers web session with the web server. A shared secret will be determined with the manufacturer along with other account information. The method of this shared secret will be determined at a later time. The manufacturer will upload the device information into the database for future device authentication, and will incorporate the appropriate identification to be relayed between the device and the database. Listed below are possible protocols that will be integrated into the database and devices to transmit and receive information:

- Transport Layer Security (TLS) provides the secure communication between the WSD and the Database in the upper layer. TLS is a cryptographic protocol that provides security for communication over networks as well as the Internet. The

Devices will act as a TLS client to communicate with the database. (See RFC 5246, RFC 4346, RFC 2246, RSA 2048/SHA-256/AES.)

5-b) It must include a description of the security methods that will be used to ensure that unauthorized parties cannot access or alter the database or otherwise corrupt the operation of the database system in performing its intended functions.

Comsearch has implemented multilayered security methodology for protecting our Internet Gateway (i.e., ingress and egress). Our IT Security Policy and Standards define technology and techniques used as part of its protection methodology. We employ technologies such as, but not limited to, firewalls, intrusion protection, and information loss prevention.

We envision that the following security methods may be employed to protect the database system:

- Database communication with other Database Providers can be handled real time using Web Services with a protocol such as SOAP. Each database provider will be required to identify themselves using certificate authentication, encrypted account login, and account password over secured Web Services. We will log each transaction received noting the specific database provider, timestamp and the other pertinent information. If an unknown database provider attempts to breach using Web Services, our security will flag and refuse the receipt of information.
- The encrypted data transfer between device and database will include, but is not limited to, device identifier, manufacturer identifier, location coordinates and the shared secret. Appropriate security protocols will be used to ensure that an

unknown device and/or party cannot access the database or perform a denial of service attack.

- The device will pass the shared secret to the database and the database will transmit the appropriate authentication response for the shared secret along with channel availability list back to the device. All communications between device and database will be recorded in the database.
- If the database determines the device is not authorized based on the shared secret, manufacturer identifier and device identifier, an error will be returned to the device. All failures will be carefully reviewed to identify, track, and report to the FCC and manufacturers any and all criminal or improper activity from a user, database manager and/or device.
- Logging onto the Web Server for registrations of fixed and manufacturer device information will be handled by our proprietary account security methods. These methods include SSL encryption on the web server with 128bit encryption in database storage. We have implemented an account lock down policy to prohibit the user from attempting login hacks. If a user attempts to login three times unsuccessfully, the account will automatically be locked. A notification of the account specifics and date-time of login attempts will be sent to the account owner and the database administrator. All account passwords will expire at a predetermined time and must be changed by the account owner. We will also prohibit use of proper words/names and the user must include alpha numeric characters. A password cannot be repeated.
- All database activity will be tracked using proprietary mechanisms already in use with our other product lines. The tracking mechanism will provide a history of all

requests via Web Services with other database providers, user web sessions and device-database activity.

- Existing back up/recovery policy includes off-site storage, redundant server/hardware, disk mirroring, monthly patch upgrades, routine database diagnostics, redundant power supply, daily database and system backups and physical disaster/recovery documentation.
- Our IT Security and Risk Management group performs periodic security assessments. These assessments occur over physical, technical, human resources and application security areas.
- All development follows strict policies ensuring discrepancy/bug tracking, source control, resolution documentation and thorough unit regression testing.

5-c) In addition, the entity should describe whether and how security methods will be used to verify that Mode I personal/portable devices that rely on another device for their geographic location information have received equipment authorization.

Comsearch does not believe the current rules for white space require that the database verify whether any devices have received equipment authorization. In our *ex parte* discussions with the Commission we stated, "The Order states clearly that the responsibility of the database is only to provide "a list of available channels on which the unlicensed device could choose to operate,"[10] and not to validate or verify white space devices beyond what is required by white spaces rules.[11] The database should not be considered a barrier to the operation of devices that might function outside of the Commission's rules."

[10] Order at ¶ 212.
[11] *Id*. at Rule Section 15.715 TV Bands Administrator.

In addition, we have not been required to verify devices' FCC authorization status in either the WMTS or 70 – 90 GHz databases. We strongly believe that if this is a requirement for verification of WSDs, the Commission must address it in the rules. Nonetheless, should the Commission require equipment authorization verification, Comsearch will support those requirements using the same methods described above.